École supérieure d'Informatique et du Commerce

Examen AIS

Nom : HASHEMI

Prénom : Said

Date : 16/05/2024

Travail à réaliser

2.1 administrer et sécuriser le réseau d'entreprise :

1. Pour améliorer notre réseau, nous allons :

Diviser en parties avec VLANs.

Utiliser une authentification centralisée.

Installer des pare-feu.

Utiliser des outils de détection.

Sécuriser le Wi-Fi avec un chiffrement fort et des réseaux distincts.

Maintenir à jour et appliquer des règles strictes.

Configurer des VPN sécurisés.

Prioriser le trafic essentiel comme la téléphonie IP.

Pour gérer la coexistence : En considérant les mesures de sécurité à implémenter mentionnées en haut, pour gérer la coexistence de différents types d'utilisateurs, j'utilise des politiques basées sur les rôles, je peux définir des permissions spécifiques à chaque type d'utilisateur, renforçant ainsi le contrôle d'accès. L'authentification 802.1X, couplée à un serveur RADIUS, permettra d'authentifier les utilisateurs de manière sécurisée. Enfin, la configuration de pare-feu internes servira à contrôler le trafic entre les VLANs et à empêcher tout accès non autorisé.

2. Pour la sécurité de Wifi, j'utilise WPA3 (Wi-Fi Protected Access 3) au lieu de WPA2-PSK pour une sécurité renforcée et une meilleure protection contre les attaques.

3. Pour renforcer la sécurité des utilisateurs nomades salariés de l'entreprise, plusieurs options d'authentification alternatives au simple login/password sont disponibles. Je peux opter pour l'authentification multi-facteurs, qui demande plusieurs méthodes d'identification pour renforcer la sécurité. L'authentification biométrique utilise des caractéristiques uniques comme les empreintes digitales ou la reconnaissance faciale. Les certificats numériques assurent une sécurité forte grâce à des clés cryptographiques. Les jetons numériques et l'authentification par appareil simplifient l'accès tout en garantissant la sécurité. En choisissant la solution qui correspond le mieux aux besoins de l'entreprise en considérant les ressources financières et matérielles disponibles, je peux assurer un accès sécurisé et pratique aux ressources réseau pour les employés nomades.

École supérieure d'Informatique et du Commerce

Examen AIS

Nom : HASHEMI

Prénom : Said

Date : 16/05/2024

2.2 administrer et gérer un environnement système hétérogène :

1. Cinq étapes simples pour renforcer la sécurité d'un contrôleur de domaine Windows :

1. Mots de passe forts : Exigez des mots de passe robustes et changez-les régulièrement pour limiter les risques d'accès non autorisés.
2. Mises à jour régulières : Assurez-vous que tous les logiciels sont à jour avec les derniers correctifs de sécurité pour protéger le système contre les menaces.
3. Surveillance des journaux : Configurez les journaux d'événements pour détecter les activités suspectes et mettez en place des alertes en cas d'incidents.
4. Chiffrement des communications : Activez le chiffrement pour sécuriser les échanges de données entre le contrôleur de domaine et les clients.
5. Sauvegardes régulières : Effectuez des sauvegardes régulières des données pour assurer une récupération en cas de besoin.

2. **Certificat Wildcard :** Le certificat wildcard est utilisé pour sécuriser plusieurs sous-domaines d'un domaine principal avec un seul certificat. Les fichiers associés comprennent :

SSLCertificateFile : Le certificat SSL pour le domaine principal (*.mondomaine.com).

SSLCertificateKeyFile : La clé privée associée au certificat.

SSLCertificateChainFile : Le fichier de chaîne de certificats, qui inclut le certificat racine et les certificats intermédiaires nécessaires pour valider le certificat SSL.

Ensemble, ces fichiers permettent d'établir une connexion sécurisée entre le serveur web et le navigateur des utilisateurs, en garantissant que les données échangées sont cryptées et protégées contre les interceptions.

3.Pour copier des fichiers Windows sur une VM Debian : j'utilise SCP (Secure Copy Protocol) pour transférer les fichiers de l'environnement de développement Windows vers le conteneur tournant sur une VM Debian dans le cloud privé.

Nom : HASHEMI

Prénom : Said

Date : 16/05/2024

2.3 Intégrer et gérer les différents équipements de travail des utilisateurs

1. proposition de deux moyens pour la confidentialité des données stockées sur les PC portables :

Chiffrement du disque dur : Je peux utiliser un logiciel de chiffrement de disque dur comme BitLocker (pour Windows) ou FileVault (pour macOS) pour crypter toutes les données stockées sur le disque dur du PC portable. En cas de perte ou de vol, les données restent illisibles sans la clé de déchiffrement.

Gestion des appareils à distance : Je mets en place une solution de gestion des appareils à distance qui permet de verrouiller et d'effacer à distance les données du PC portable en cas de perte ou de vol. Par exemple, Microsoft Intune ou Jamf Pro (pour les appareils macOS) offrent ces fonctionnalités.

2. Trois règles élémentaires et bonnes pratiques pour un administrateur afin de sécuriser les postes mobiles sont :

1. Mises à jour régulières : Il faut s'assurer que les systèmes d'exploitation, les applications et les logiciels tiers sur les postes mobiles sont toujours à jour avec les derniers correctifs de sécurité pour réduire les vulnérabilités potentielles exploitées par les attaquants.
2. Utilisation d'un antivirus/antimalware : Je dois installer et maintenir à jour un logiciel antivirus ou antimalware sur les postes mobiles pour détecter et supprimer les menaces potentielles, telles que les virus, les logiciels malveillants et les programmes indésirables.
3. Politiques de sécurité strictes : Il faut que je définisse et applique des politiques de sécurité strictes pour les postes mobiles, telles que des exigences de mots de passe forts, des limites d'accès basées sur les rôles, l'activation du chiffrement des données et la restriction des téléchargements d'applications non autorisées.

3. En quelques lignes :

Un système de gestion de la mobilité (MDM) assure la gestion centralisée des appareils mobiles, notamment leur configuration, sécurité et déploiement d'applications. Il répond aux problématiques de sécurisation des données, gestion des appareils, et respect des politiques de conformité. Un exemple de produit est VMware Workspace ONE UEM.

4. Pour utiliser des tablettes Android avec une authentification via un annuaire centralisé, suivez ces étapes simples :

Configuration de l'annuaire centralisé : Je m'assure que votre annuaire (comme Active Directory) est correctement configuré avec les comptes utilisateurs.

Paramètres de sécurité sur les tablettes : Activation l'authentification via l'annuaire centralisé dans les paramètres de sécurité des tablettes Android.

Nom : HASHEMI

Prénom : Said

Date : 16/05/2024

Connexion au réseau : Il faut s'assurer que les tablettes sont connectées au réseau de l'entreprise.

Configuration des paramètres d'authentification : Je dois configurer les paramètres d'authentification sur les tablettes pour utiliser l'annuaire centralisé.

Test

2.4 Superviser, mesurer les performances et la disponibilité de l'infrastructure et en présenter les résultats

1. indicateurs de supervisons et alarmes sur le FW : Je surveille le trafic réseau, les connexions simultanées, les logs d'événements, les mises à jour du firmware, les règles du pare-feu et l'utilisation des ressources pour détecter les menaces et les erreurs de configuration sur le pare-feu.

2. La principale différence entre SNMPv2 et SNMPv3 est la sécurité. SNMPv3 offre des fonctionnalités de sécurité avancées comme l'authentification et le chiffrement, tandis que SNMPv2 ne le fait pas.

3. pour assurer la supervision des environnements cloud/hybrides :

- API de surveillance : Les fournisseurs cloud offrent souvent des API pour surveiller les performances et l'utilisation des ressources.
- Agents de surveillance : Certains fournisseurs proposent des agents logiciels installés sur les machines virtuelles pour collecter des données de surveillance.
- Intégration avec des outils existants : Les outils de supervision traditionnels peuvent être adaptés aux environnements cloud/hybrides pour collecter et analyser les données.
- Solutions tierces spécialisées : Il existe des solutions de surveillance dédiées aux environnements cloud/hybrides, offrant une surveillance complète et adaptée.

École supérieure d'Informatique et du Commerce

Examen AIS

Nom : HASHEMI

Prénom : Said

Date : 16/05/2024

2.5 Mesurer et analyser le niveau de sécurité de l'infrastructure

1. Je recommande des outils comme indiqué ci-dessous pour évaluer la vulnérabilité d'un site web lors d'un audit passif :

1. Scanners de vulnérabilités : Pour détecter les failles connues comme les injections SQL ou les failles XSS.
2. Analyseurs de logs : Pour repérer les tentatives d'accès non autorisées et les activités suspectes dans les journaux du serveur web.
3. Sniffeurs réseau : Pour détecter les anomalies et les comportements suspects dans le trafic réseau.
4. Proxies HTTP/HTTPS : Pour intercepter et analyser le trafic web à la recherche de vulnérabilités.
5. Analyseurs de trafic web : Pour surveiller en temps réel les comportements anormaux et les attaques en cours.

2. Dans un audit de sécurité, quatre éléments essentiels à inclure sont :

1. Évaluation des risques : Identifier et évaluer les menaces potentielles, les vulnérabilités et les impacts sur la sécurité des systèmes et des données.
2. Analyse des politiques et des procédures de sécurité : Examiner les politiques, les procédures et les pratiques de sécurité en place pour s'assurer qu'elles sont adéquates et conformes aux normes de sécurité.
3. Test de sécurité : Effectuer des tests techniques tels que des analyses de vulnérabilités, des tests d'intrusion et des audits de configuration pour détecter les faiblesses potentielles dans les systèmes et les réseaux.
4. Rapport et recommandations : Fournir un rapport détaillé des constatations de l'audit, y compris les risques identifiés, les lacunes de sécurité et les recommandations pour améliorer la posture de sécurité globale.

3. Dans le SI de l'entreprise Omega, deux éléments essentiels sont le système de gestion des données client et l'infrastructure réseau et sécurité. Le système de gestion des données client est crucial pour les opérations commerciales, tandis que l'infrastructure réseau et sécurité garantit la connectivité et la protection des données. Les biens essentiels sont vitaux pour l'entreprise, tandis que les biens de support sont nécessaires mais pas aussi critiques pour son fonctionnement.

4. **Un événement redouté** est une situation critique qui pourrait causer des dommages importants à une entreprise. Il est défini en fonction de son impact significatif, de sa probabilité élevée et de ses conséquences multiples. Par exemple, une cyberattaque majeure compromettant les données sensibles de l'entreprise serait un événement redouté en raison de ses conséquences financières, de sa probabilité et de ses répercussions sur la réputation.

École supérieure d'Informatique et du Commerce

Examen AIS

Nom : HASHEMI

Prénom : Said

Date : 16/05/2024

2.6 Participer à l'élaboration et à la mise en œuvre de la politique de sécurité

1. Pour éviter toute utilisation indésirable du wifi invité, je peux faire :

Authentification : Mettre en place une authentification par code d'accès temporaire ou par SMS.

Limitation des ressources : limiter la bande passante et le nombre de connexions simultanées.

Surveillance : utiliser des outils de surveillance pour suivre l'utilisation du wifi invité.

Expiration automatique : configurer des sessions avec une durée limitée.

Politiques d'utilisation : définir des politiques claires et informez les utilisateurs.

Pour suivre ces mesures, utiliser des outils de gestion de réseau et des rapports détaillés sur l'utilisation du wifi invité.

2. Pour assurer une haute disponibilité des services sur les serveurs gérés par ESN, j'utiliserais Docker et Kubernetes. Docker permet de créer des conteneurs isolés pour chaque service, tandis que Kubernetes orchestre ces conteneurs pour assurer une répartition de charge et une reprise sur incident automatique, garantissant ainsi une disponibilité continue des services.

3. 10 principes simples de sécurité pour les utilisateurs nomades sont :

1. Utiliser des mots de passe forts et uniques.
2. Mettre à jour régulièrement les logiciels.
3. Privilégier les connexions Wi-Fi sécurisées.
4. Chiffrer les données sensibles.
5. Sauvegarder les données régulièrement.
6. Être vigilant face aux menaces comme le phishing.
7. Verrouiller les appareils lorsqu'ils ne sont pas utilisés.
8. Utiliser un VPN pour une connexion sécurisée.
9. Éviter les périphériques non sécurisés.
10. Signaler tout incident de sécurité à l'équipe informatique.